IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	000479.00001
Mark M. Stephenson, et al.			
Serial No.:	09/824,132	Group Art Unit:	2145
Filed:	April 3, 2001	Examiner:	Bhatia, Ajay M.
For:	System and Method for Projecting Content Beyond Firewalls	Confirmation No.:	8931

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Service Window
Mail Stop - Appeal
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

This is an Appeal Brief filed in support of Appellants' September 18, 2007, Notice of Appeal. Appeal is taken from the Final Office Action mailed July 24, 2007 (hereafter, "Final Office Action").

Please charge any fees to our Deposit Account No. 19-0733. In addition, any extensions of time necessary for acceptance or entry of this paper are hereby requested.

REAL PARTY IN INTEREST

37 C.F.R. § 41.37(c)(1)(i)

The owner of this application, and the real party in interest, is Science Applications International Corporation (SAIC) of San Diego, California.

RELATED APPEALS AND INTERFERENCES

37 C.F.R. § 41.37(c)(1)(ii)

There are no related appeals or interferences.

STATUS OF CLAIMS

37 C.F.R. § 41.37(c)(1)(iii)

Claims 55-81 are pending and stand rejected. Claims 1-54 have been canceled. Appellants hereby appeal the rejection of claims 55-81.

STATUS OF AMENDMENTS

37 C.F.R. § 41.37(c)(1)(iv)

No amendments were filed after the Final Rejection mailed on July 24, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

37 C.F.R. § 41.37(c)(1)(v)

In making reference herein to various embodiments in the specification text and/or drawings to explain the claimed invention, Appellants do not intend to limit the claims to those embodiments; all references to the specification and drawings are illustrative unless otherwise explicitly stated.

Two computers each protected behind separate firewalls cannot easily exchange data over a network because the firewalls hide the computers from each other. Although HTTP allows bi-directional communication between a computer behind a firewall and an HTTP server on the other side of the firewall, HTTP does not allow generalized communication between two computers each protected by a firewall because HTTP follows a client/server communication paradigm (i.e., one computer must act as the client, the other as the server). Page 1, lines 18-24 to page 2, line 6, paragraph [05]. Requiring that the firewalls be modified to accommodate communication is cumbersome and undesirable, since system administrators must be involved in the process and must make changes to the firewalls, and the resulting changes can compromise security. Page 2, lines 7-18 (paragraph [06]).

According to various embodiments of the invention, an intermediate computer located between the two firewalls is configured to create connections between two endpoint computers, wherein each endpoint initiates a connection with the intermediate computer. In this way, the intermediate computer enables the two computers to communicate bi-directionally as if they are connected together over the same private network without the need to modify either firewall.

Page 7, lines 15-22 (paragraph [35]). Four independent claims on appeal recite features of this approach.

Independent Claim 55

Independent claim 55 recites a method of communicating between computers, comprising the steps of:

(1) transmitting from a first computer (FIG. 1, client 101) to an intermediate server computer (FIG. 1, server 107) a first HTTP POST message through a firewall (FIG. 1, firewall 106, page 7 lines 1-14) that is open to outbound Internet traffic (page 6 lines 12-19, paragraph [33]), wherein the first HTTP POST message requests establishment of a connection between the first computer and the intermediate server computer over a first return path (FIG. 5A, step 506, page 7 lines 1-14, paragraph [34], page 22 lines 1-27, paragraphs [106] to [107]);

(2) receiving from the intermediate server computer a response including a connection identifier corresponding to the first return path (FIG. 5A, step 507, page 21, lines 9-12, paragraph [103], page 22 lines 1-27, paragraphs [106] and [107]);

(3) periodically transmitting from the intermediate server computer to the first computer a "keep alive" message over the first return path, if no further messages are sent to the first computer within a period of time (page 13 lines 6-8, paragraph [61], page 23 lines 1-10);

(4) exchanging encryption keys between the first computer and the intermediate server computer (FIG. 5A, step 508, page 13 lines 16-24, paragraph [63], page 24 lines 2-10);

(5) repeating steps (1) through (4) between a second computer (FIG. 1, client 115) and the intermediate server computer (FIG. 1, server 107, through second firewall 113), thereby creating a second return path between the second computer and the intermediate server computer (FIG. 5B, step 512 , page 27 lines 3-7, page 7 lines 1-14, paragraph [34]);

(6) transmitting encrypted information from the first computer through the firewall to the intermediate server computer using further HTTP POST messages (FIG. 5C, step 514; page 3 lines 8-12, paragraph [08], page 8 lines 17-24, paragraph [40]); and

(7) transmitting the encrypted information from the intermediate server over the second return path (FIG. 5C, step 516, page 3 lines 8-12, paragraph [08], page 7 lines 11-14, paragraph [34], page 8 lines 17-24, paragraph [40]).

Independent Claim 57

Independent method claim 57 recites a method of communicating between a first computer (FIG. 1, client 101) protected by a first firewall (FIG. 1, firewall 106) and a second computer (FIG. 1, client 115) protected by a different second firewall (FIG. 1, firewall 113), from the perspective of an intermediate third computer (FIG. 1, server 107), comprising the steps of:

(1) at a third computer (FIG. 1, server 107) situated between the first firewall and the different second firewall, receiving a first HTTP message (FIG. 5A, step 506, page 7 lines 1-14, paragraph [34]) from the first computer through a first firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic (page 6 lines 12-19, paragraph [33], page 7 lines 1-14, paragraph [34]);

(2) from the third computer, sending a first response message to the first computer through the first firewall, thereby establishing a first receive channel through the first firewall (page 22, lines 1-27, paragraphs [106] and [107]), wherein the first response message is linked to the first HTTP message (page 22 lines 19-22, paragraph [107]);

(3) at the third computer, receiving a second HTTP message from the second computer through a different second firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic (FIG. 5B, step 512, page 7 lines 1-14, paragraph [34]);

(4) from the third computer, sending a second response message to the second computer through the second firewall, thereby establishing a second receive channel through the second firewall, wherein the second response message is linked to the second HTTP message (FIG. 5B, step 512, page 7 lines 1-14, paragraph [34]);

(5) at the third computer, receiving a third encrypted HTTP message from the first computer through the first firewall; determining that the third encrypted HTTP message is intended to be delivered to the second computer, and transmitting to the second computer the third encrypted HTTP message, wherein the third encrypted HTTP message is transmitted over the second receive channel through the second firewall to the second computer (FIG. 5C, steps 514, 516, page 3 lines 8-12, paragraph [08], page 7 lines 11-14, paragraph [34], page 8 lines 17-24, paragraph [40]; page 28 lines 12-27); and

(6) from the third computer, periodically transmitting "keep alive" messages to the first computer over the first receive channel and to the second computer over the second receive channel to avoid a time-out condition (page 13 lines 6-8, paragraph [61], page 23 lines 1-10).

Independent Claim 66

Independent method claim 66 recites a method of communicating between a first computer (FIG. 1, client 101) protected by a first firewall (FIG. 1, firewall 106, page 7 lines 1-14) and a second computer (FIG. 1, client 115) protected by a different second firewall (FIG. 1, 113) via a third intermediate computer (FIG. 1, server 107), comprising the steps of:

receiving at the third intermediate computer (FIG. 1, server 107, page 7 lines 1-14, FIG. 5A, step 506, page 7 lines 1-14, paragraph [34]) a request transmitted from the second computer through the second firewall, wherein the request is to establish a receive channel (page 22, lines 1-15) between the second computer and the third intermediate computer;

transmitting from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions by the third intermediate computer (FIG. 5A, step 507, page 22 lines 16-27);

receiving at the third intermediate computer data transmitted from the first computer through the first firewall via a network connection initiated by the first computer (FIG. 5C, step 514, page 3 lines 8-12, paragraph [08], page 8 lines 17-24, paragraph [40]);

determining that the data received from the first computer is intended to be delivered to the second computer (FIG. 5C, steps 514, 516, page 28 lines 9-16, paragraphs [139] and [140]); and

transmitting the data to the second computer via the receive channel (FIG. 5C, step 516, page 28 lines 27-28 to page 29 lines 1-6, paragraph [142]).

Independent Claim 74

Independent method claim 74 recites a method of communicating between a first computer (FIG. 1, client 101) protected by a first firewall (FIG. 1, firewall 106, page 7 lines 1-14) and a second computer (FIG. 1, client 115) protected by a different second firewall (FIG. 1 firewall 113) via a third intermediate computer (FIG. 1, server 107), from the perspective of the second computer (FIG. 1, client 115), comprising the steps of:

transmitting a request from the second computer (FIG. 1, client 115) to the third intermediate computer (FIG. 1, server 107) through the second firewall (FIG. 1, firewall 113) to establish a receive channel between the third intermediate computer and the second computer (page 7 lines 1-14, FIG. 5A, step 506, page 22, lines 19-22);

receiving from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions from the third intermediate computer (FIG. 5A, steps 507, page 22 lines 1-15); and

receiving data via the receive channel, wherein the data was transmitted from the first computer to the third intermediate computer through the first firewall via a network connection initiated by the first computer, then transmitted from the third intermediate computer to the second computer via the receive channel (FIG. 5C, step 514, page 3 lines 8-12, paragraph [08], page 8 lines 17-24, paragraph [40], page 28 lines 27-28 to page 29 lines 1-6, paragraph [142])..

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

37 C.F.R. § 41.37(c)(1)(vi)

Claims 55-81 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Alden et al. (U.S. Patent No. 6,101,543) in view of Erickson et al. (U.S. Patent No. 6,412,009). According to the office action, Alden discloses transmitting messages through two firewalls separating three computers, but it does not disclose the use of HTTP POST messages or the "keep alive" feature recited in the independent claims. According to the office action, Erickson discloses those features.

ARGUMENT

37 C.F.R. § 41.37(c)(1)(vii)

A. Rejection of Independent Claim 55

Independent claim 55 recites transmitting encrypted information from a first computer to an intermediate server computer through a firewall, and then "transmitting the encrypted information from the intermediate server over the second return path," to a second computer. Alden discloses intermediate servers as part of a network tunnel, but does not teach or suggest the establishment of a return path established via an HTTP POST operation as claimed or the

transmission of data over a return path, as recited in claim 55. As discussed in the Amendment filed October 19, 2006, the data transmitted from Alden's intermediate tunnel servers to the tunnel endpoints is transmitted directly through the firewall. (Alden, col. 6, lines 24-67.) In other words, Alden does not transmit data over a "return path," as recited in claim 55. Rather, Alden transmits directly into the firewalls protecting the tunnel endpoints, thus requiring these firewalls to be "programmed to pass packets received over transport layer connection 2 into a private network on the other side of the firewall." (Alden, col. 6, lines 37-39.).

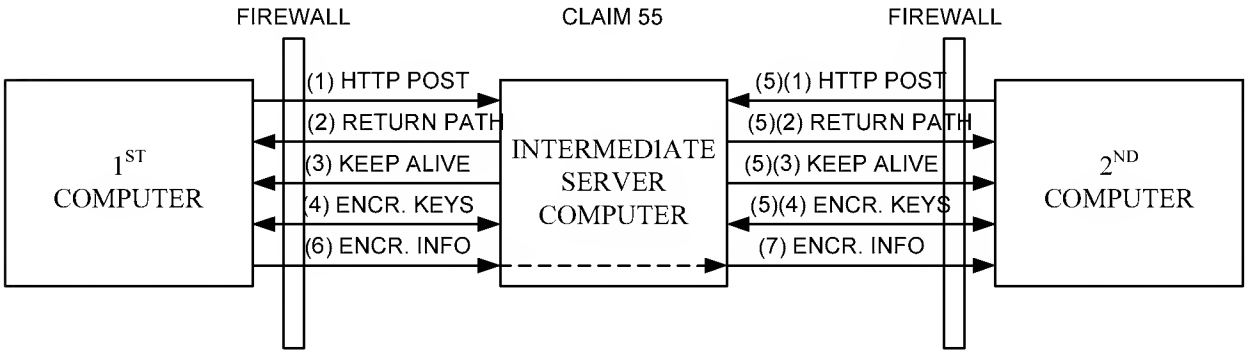
The Office Action alleges that transmitting encrypted information from an intermediate server over a return path to a recipient is disclosed by Alden at col. 8, lines 45-67. The relied-upon portion of Alden relates to transmitting a request frame and a response frame over a previously established transport layer connection, to communicate key encryption and authentication information between the tunnel endpoints. However, Alden's previously established transport layer connection involves transmitting data directly to the pre-programmed firewall, rather than establishing or transmitting via a return path as claimed. (Alden, col. 6, lines 24-67.) Thus, Alden's request and response frames are not sent over a "return path," as recited in claim 55. Accordingly, Applicants submit that Alden does not teach or suggest transmitting encrypted information from a first computer to an intermediate server computer through a firewall, and then "transmitting the encrypted information from the intermediate server over the second return path," as recited in claim 55.

Nor does Erickson teach or suggest transmitting encrypted information from an intermediate server to a recipient computer over a return path, as recited in claim 55. At most, Erickson discloses communicating between a single web client and web server through port 80 in a firewall (col. 5 lines 47-67). It does not disclose or suggest creating two separate return paths (recited in steps (1), (2) and (5) of claim 55), followed by transmitting information from the first computer through an intermediate server computer to a second computer over the return paths created by two HTTP POST messages as recited in claim 55.

Additionally, claim 55 respectively recites in steps (1) and (5) that the first and the second computer each transmit a request to establish a connection with the intermediate server computer. In other words, the two endpoints initiate connections (creating "return paths") with the intermediate server using HTTP POST messages. In contrast, Alden only describes

techniques in which one endpoint computer of the network tunnel initiates communications via the tunnel servers, and the other endpoint computer is a passive recipient. (See Alden, FIG. 3; col. 6, lines 24-67.) Similarly, Erickson describes a web client initiating communications to a web server via a tunneling mechanism. (Erickson, col. 3, lines 3-29). However, Erickson does not teach or suggest any configuration in which two different computers initiate communications with a third intermediate server as claimed.

The following figure shows the steps of independent method claim 55, with numbered steps keyed to message flows:



As can be seen, the first and second computer each initiate an HTTP POST message, resulting in a return path to each respective computer. Return means "going back to." Each return path is kept open through the firewall by periodic keep-alive messages. In contrast, Alden clearly shows in FIG. 3 and FIG. 4 that one network endpoint initiates a tunnel all the way through the other endpoint – the other endpoint does not request a connection resulting in any "return path" to that endpoint.

As shown below in FIG. 3 of Alden, Alden's tunnel originates at tunnel server A (element 46) and traverses the two firewalls all the way to tunnel server D (element 62).

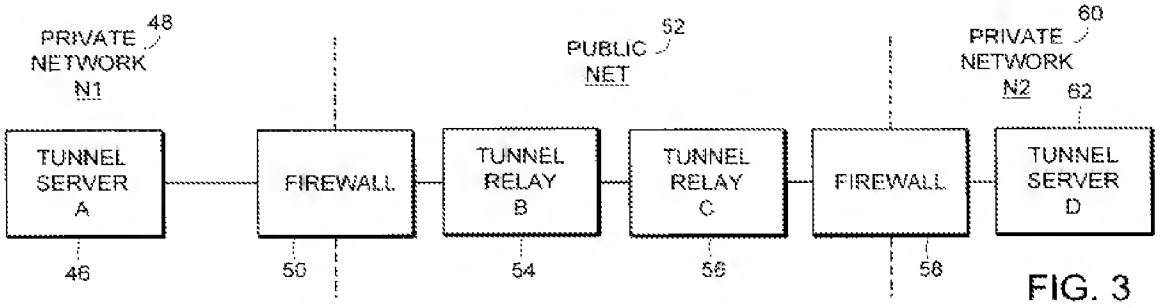


FIG. 3

This is confirmed by the FIG. 4 flowchart of Alden, which clearly shows that the tunnel is created entirely by the leftmost node in the network, which only receives a response from the other endpoint (tunnel server D):

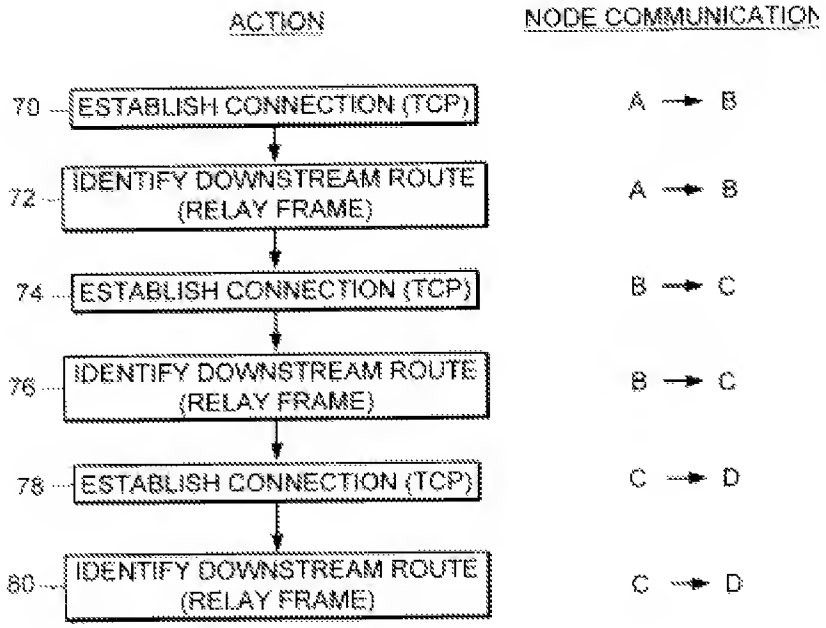


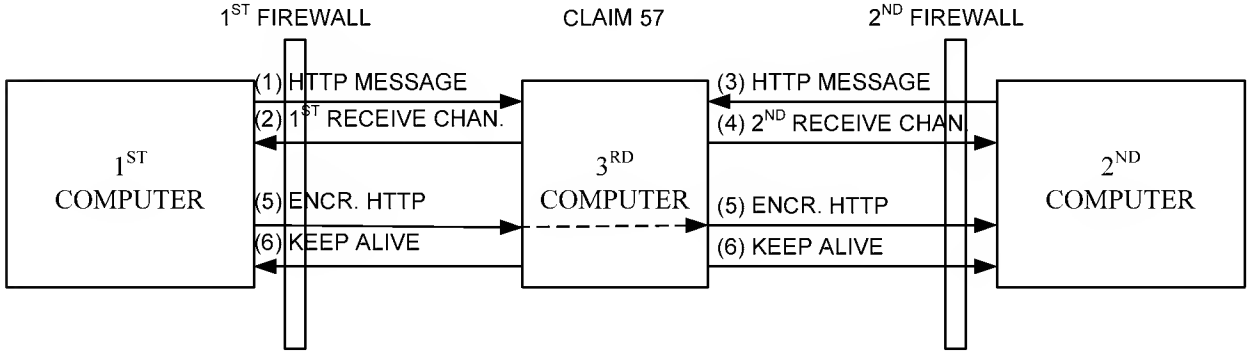
FIG. 4

Clearly, nothing in Alden or Erickson discloses or suggests the creation of two return paths requested by two different computers and then transmitting data from the first computer to the second computer over the second return path as recited in independent claim 55. Even assuming that Alden and Erickson are combined as suggested by the examiner, the claimed method would not result. Accordingly, claim 55 cannot properly be rejected based on Alden even in combination with Erickson.

Moreover, independent claim 55 recites in step (2) that a response is received from the intermediate server computer "including a connection identifier corresponding to the first return path." Similarly, step (5) recites the repetition of step (2) between a second computer and the intermediate server computer, thus also "including a connection identifier corresponding to the [second] return path." Neither Alden nor Erickson discloses receiving connection identifiers in response to HTTP POST messages as recited in claim 55.

B. Rejection of Independent Claim 57

Independent claim 57 recites a method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall using a third intermediate computer situated between the two firewalls, wherein an encrypted HTTP message from the first computer is received by the third computer and transmitted over a "receive channel" to the second computer. The term "receive channel" is defined in the specification on page 13, lines 3-6, paragraph [61] as follows: "A receive channel is a response to a post from the client that is opened by the server and may remain open until the communication is discontinued. This receive channel allows the server to send data to the client at any time." The claim further requires sending first and second HTTP messages (each respectively sent by the first and second computers) through respective firewalls that are configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic. Clearly, the claim requires the establishment of two "receive channels" (each defined as a response to a post from the client that is opened by the server and remains open until the communication is discontinued), one between the first computer and intermediate computer, and a second one between the second computer and the intermediate computer, and then transmitting an encrypted HTTP message from the first computer to the second computer through the intermediate third computer via the second receive channel. The following diagram corresponds to the steps of independent claim 57:

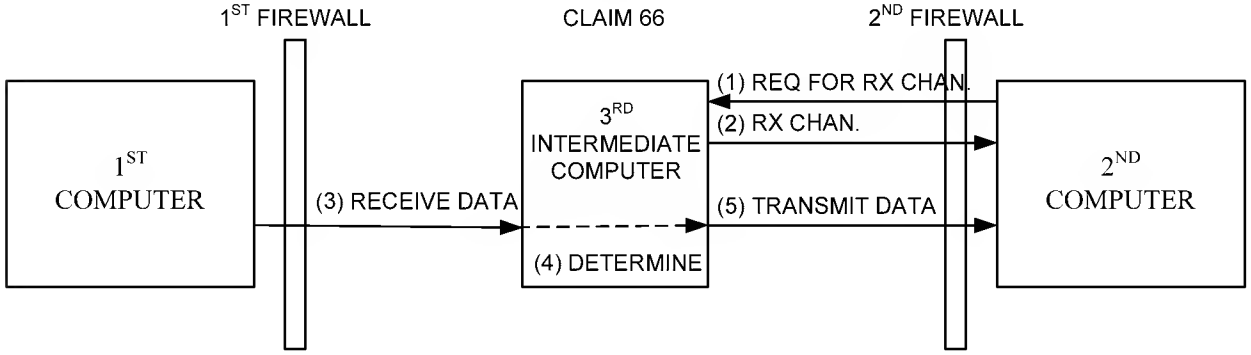


As explained above, neither Alden nor Erickson describes or suggests the creation of two receive channels initiated by the computer endpoints and then transmitting encrypted HTTP data from the first computer to the second computer through the intermediate computer over the

second receive channel as claimed. Nowhere does the office action address this feature. Accordingly, the rejection is improper.

C. Rejection of Independent Claims 66 and 74

Independent claim 66 recites, as its first step, "receiving at the third intermediate computer a request . . . to establish a receive channel between the second computer and the third intermediate computer" and then, as its second step, "transmitting . . . a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer . . ." As explained above, a "receive channel" is defined in the specification (page 13, lines 3-6, paragraph [61]) as "a response to a post from the client that is opened by the server and may remain open until the communication is discontinued. This receive channel allows the server to send data to the client at any time." The claim further requires receiving data transmitted from the first computer through the first firewall, determining that it is intended to be delivered to the second computer, and then transmitting the data to the second computer via the receive channel. The diagram below illustrates the steps of claim 66:



The office action brushes aside this claim with the statement that "Claims 61-81 list all the same elements of claims 55-60. Therefore, the supporting rationale of the rejection to claims 55-60 applies equally as well to claims 61-81." (Final Office Action at page 7).

Neither Alden nor Erickson, even in combination, discloses or suggests receiving data through a first firewall from a first computer and sending it to a second computer through a second firewall using a receive channel previously established by the second computer, as recited in independent claim 66. Alden merely discloses tunneling through two firewalls, wherein the tunnel is created by one endpoint. Erickson merely discloses sending data through a single firewall using HTTP. Accordingly, this rejection is unfounded.

Independent claim 74 is similar to independent claim 66 (i.e., it requires similar actions), but it is written from the perspective of one of the endpoint computers (i.e., it recites actions occurring in one of the endpoint computers), whereas independent claim 66 is written from the perspective of the intermediate computer (i.e., it recites actions occurring in the intermediate server computer). Although the scope of the claims is not identical, the rejection of independent claim 74 is improper for the same reasons outlined above for claim 66 – namely, the creation of a receive channel (defined in the specification) followed by the receipt, through an intermediate computer over the "receive channel," of data from a first computer, thus traversing two firewalls each protecting one of the two endpoint computers.

D. Rejection of Dependent claim 56

As explained on page 16 of Applicants' Amendment filed October 19, 2006, claim 56 recites, "in the intermediate server computer, decrypting encrypted information received from the first computer using encryption keys shared between the first computer and the intermediate computer, and then re-encrypting the received information using encryption keys shared between the intermediate computer and the second computer." The Final Office Action alleges that Alden teaches this feature at col. 8, lines 45-67, the same allegation that was cut-and-pasted from the non-final office action mailed on March 7, 2007. However, the only encryption disclosed by Alden takes place between the two endpoints of the tunnel connection. See Alden, col. 8, lines 31-56; col. 10 lines 12-15; col. 13 line 42 to col. 14 line 10. Thus, Alden does not teach or suggest an intermediate server "decrypting encrypted information" using encryption keys shared between the first and intermediate computers as recited in claim 56. Neither the Final Office action nor the office action mailed on March 7, 2007 ever addressed Applicants' argument, which was made in the October 19, 2006 response.

E. Rejection of Dependent Claim 59

Dependent claim 59 recites:

> 59. The method of claim 55, wherein at least one of the HTTP POST messages transmitted during step (6) comprises an identifier of said second computer encrypted with a first encryption key associated with the intermediate server, and wherein said encrypted information is encrypted with a second different encryption key associated with the second computer.

The Final Office Action (page 7) alleges that this feature is disclosed in Erickson at col. 5 lines 43-42 [sic], col. 8 at lines 20-40, and FIG. 5, and in Alden at col. 8, lines 45-67. Nowhere can this feature be found in the portions cited by the Final Office Action. The word "encryption" appears nowhere in the entire Erickson patent. Alden only discusses encryption between endpoints, not between any intermediate servers as claimed. Nor does Alden disclose use of two encryption keys, one associated with the intermediate server and used to encrypt the identifier of the second computer and the other associated with the second computer and used to encrypt the information from the first computer that is sent to the second computer. Accordingly, the rejection of this claim is improper.

F. Rejection of Dependent Claim 60

Dependent claim 60 recites:

> 60. The method of claim 57, wherein the third encrypted HTTP message comprises:
>
> an encrypted identifier of the second computer, the identifier encrypted with a first encryption key associated with the third computer, and
>
> encrypted content for delivery to the second computer, the content encrypted with a different second encryption key associated with the second computer.

The Final Office Action states on page 7 that this feature is shown in the same portions of Erickson and Alden identified for claim 59. As pointed out above, the word "encryption" appears nowhere in Erickson, and Alden only discloses encryption between the tunnel endpoints, not between the recited third computer, which is between the first and second computers (as recited in parent claim 57). Consequently, the rejection of this claim is improper.

G. Rejection of Dependent Claim 63

Dependent claim 63 recites:

> 63. The method of claim 55, wherein communication between the first computer and the intermediate server computer is initiated by the first computer, and wherein communication between the second computer and the intermediate server computer is initiated by the second computer.

This claim clearly requires that the communication between the two communicating computers (the recited "first computer" and "second computer") and the intermediate server

computer be initiated by the first and second computers respectively. As explained above with respect to claim 55, in Alden only one computer initiates the tunnel, and the second endpoint computer is a passive recipient (i.e., it does not "initiate" the connection with the other computers). The Final Office Action dismissed this claim without any explanation or comment, despite the fact that Applicants' response filed June 5, 2007 argued that neither Alden nor Erickson describe any technique in which both of the communication endpoints initiate communication with an intermediate server as claimed. This rejection cannot be sustained.

H. Rejection of Dependent Claim 70

Dependent claim 70 recites:

> 70. The method of claim 66, wherein the data received from the first computer comprises an HTTP message encrypted using encryption keys shared between the first computer and the third intermediate computer, and wherein the third intermediate computer decrypts the HTTP message received from the first computer and re-encrypts the HTTP message using encryption keys shared between the third intermediate computer and the second computer.

This claim recites that the intermediate computer decrypts the HTTP message and then re-encrypts it using encryption keys shared between the intermediate computer and the second computer. The Final Office action dismissed this claim without any comment. As explained above, the word "encryption" appears nowhere in Erickson, and Alden merely discloses encryption between two tunnel endpoints, not any intermediate computers as recited in claim 70. Accordingly, the rejection of this claim is erroneous.

I. Rejection of Dependent Claims 72 and 80

Dependent claim 72 recites the following:

> 72. The method of claim 66, wherein communication between the first computer and the third intermediate computer is initiated by the first computer, and wherein communication between the second computer and the third intermediate computer is initiated by the second computer.

Dependent claim 80 recites the same limitation but it depends instead from independent claim 74, which was argued together with independent claim 66 above. These claims clearly require that the communication between the two communicating computers (the recited "first computer" and "second computer") and the intermediate server computer be initiated by the first

and second computers respectively. As explained above with respect to claim 55, in Alden only one computer initiates the tunnel, and the second endpoint computer is a passive recipient (i.e., it does not "initiate" the connection with the other computers). The Final Office Action dismissed these claims without any explanation or comment, despite the fact that Applicants' response filed June 5, 2007 argued that neither Alden nor Erickson describe any technique in which both of the communication endpoints initiate communication with an intermediate server as claimed. This rejection cannot be sustained.

J. Rejection of Dependent Claim 78

Dependent claim 78 recites:

> 78. The method of claim 74, wherein the data received via the receive channel comprises an HTTP message from the first computer, the HTTP message encrypted using encryption keys shared between the third intermediate computer and the second computer.

The Final Office Action dismissed this claim without any explanation. As explained above, however, the word "encryption" appears nowhere in Erickson, and Alden only discloses encryption between tunnel endpoints, not encryption between the intermediate computer and the second computer. Accordingly, the rejection is improper.

CONCLUSION

For all of the foregoing reasons, Appellants respectfully submit that the final rejection of claims 55-81 is improper and should be reversed.

Respectfully submitted,
BANNER & WITCOFF, LTD.

Dated: November 19, 2007

By: /Bradley C. Wright/
Bradley C. Wright
Registration No. 38,061

1100 13th Street, N.W.
Suite 1200
Washington, D.C. 20005
Tel: (202) 824-3000
Fax: (202) 824-3001

CLAIMS APPENDIX

37 C.F.R. § 41.37(c)(1)(viii)

Claims involved in the appeal:

55. A method of communicating between computers, comprising the steps of:

(1) transmitting from a first computer to an intermediate server computer a first HTTP POST message through a firewall that is open to outbound Internet traffic, wherein the first HTTP POST message requests establishment of a connection between the first computer and the intermediate server computer over a first return path;

(2) receiving from the intermediate server computer a response including a connection identifier corresponding to the first return path;

(3) periodically transmitting from the intermediate server computer to the first computer a "keep alive" message over the first return path, if no further messages are sent to the first computer within a period of time;

(4) exchanging encryption keys between the first computer and the intermediate server computer;

(5) repeating steps (1) through (4) between a second computer and the intermediate server computer, thereby creating a second return path between the second computer and the intermediate server computer;

(6) transmitting encrypted information from the first computer through the firewall to the intermediate server computer using further HTTP POST messages ; and

(7) transmitting the encrypted information from the intermediate server over the second return path.

56. The method of claim 55, further comprising the steps of, in the intermediate server computer, decrypting encrypted information received from the first computer using encryption keys shared between the first computer and the intermediate computer, and then re-encrypting the received information using encryption keys shared between the intermediate computer and the second computer.

57. A method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall, comprising the steps of:

(1) at a third computer situated between the first firewall and the different second firewall, receiving a first HTTP message from the first computer through a first firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic;

(2) from the third computer, sending a first response message to the first computer through the first firewall, thereby establishing a first receive channel through the first firewall, wherein the first response message is linked to the first HTTP message;

(3) at the third computer, receiving a second HTTP message from the second computer through a different second firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic;

(4) from the third computer, sending a second response message to the second computer through the second firewall, thereby establishing a second receive channel through the second firewall, wherein the second response message is linked to the second HTTP message;

(5) at the third computer, receiving a third encrypted HTTP message from the first computer through the first firewall; determining that the third encrypted HTTP message is intended to be delivered to the second computer, and transmitting to the second computer the third encrypted HTTP message, wherein the third encrypted HTTP message is transmitted over the second receive channel through the second firewall to the second computer; and

(6) from the third computer, periodically transmitting "keep alive" messages to the first computer over the first receive channel and to the second computer over the second receive channel to avoid a time-out condition.

58. The method of claim 57, wherein step (5) is performed at the third computer by transmitting the third encrypted HTTP message to the second computer without decrypting contents of the third encrypted HTTP message.

59. The method of claim 55, wherein at least one of the HTTP POST messages transmitted during step (6) comprises an identifier of said second computer encrypted with a first

encryption key associated with the intermediate server, and wherein said encrypted information is encrypted with a second different encryption key associated with the second computer.

60. The method of claim 57, wherein the third encrypted HTTP message comprises:

an encrypted identifier of the second computer, the identifier encrypted with a first encryption key associated with the third computer, and

encrypted content for delivery to the second computer, the content encrypted with a different second encryption key associated with the second computer.

61. The method of claim 56, wherein the encrypted information decrypted by the intermediate server computer comprises encrypted header information.

62. The method of claim 61, wherein the encrypted header information comprises one or more of an encrypted IP address, an encrypted username of said second computer, an encrypted header length, an encrypted message length, an encrypted application identifier, an encrypted time and date stamp, and an encrypted message type.

63. The method of claim 55, wherein communication between the first computer and the intermediate server computer is initiated by the first computer, and wherein communication between the second computer and the intermediate server computer is initiated by the second computer.

64. The method of claim 55, wherein the first firewall and the second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages initiated by a computer inside the firewall.

65. The method of claim 55, wherein periodically transmitting a “keep alive” message over the first return path comprises transmitting a “keep alive” message prior to a firewall timeout period to prevent the firewall from blocking traffic on the first receive path.

66. A method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall via a third intermediate computer, comprising the steps of:

receiving at the third intermediate computer a request transmitted from the second computer through the second firewall, wherein the request is to establish a receive channel between the second computer and the third intermediate computer;

transmitting from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions by the third intermediate computer;

receiving at the third intermediate computer data transmitted from the first computer through the first firewall via a network connection initiated by the first computer;

determining that the data received from the first computer is intended to be delivered to the second computer; and

transmitting the data to the second computer via the receive channel.

67. The method of claim 66, wherein the request comprises a message transmitted using a secure socket layer (SSL) protocol, a file transfer protocol (FTP), a HyperText Transfer Protocol (HTTP), or an electronic mail protocol.

68. The method of claim 66, wherein the request comprises an HTTP POST message transmitted through the second firewall to port 80 or port 8080.

69. The method of claim 66, wherein the data received from the first computer comprises an HTTP message encrypted using encryption keys shared between the first computer and the second computer, and wherein the third intermediate computer does not decrypt the encrypted HTTP message.

70. The method of claim 66, wherein the data received from the first computer comprises an HTTP message encrypted using encryption keys shared between the first computer and the third intermediate computer, and wherein the third intermediate computer decrypts the HTTP

message received from the first computer and re-encrypts the HTTP message using encryption keys shared between the third intermediate computer and the second computer.

71. The method of claim 70, wherein decrypting the HTTP message comprises decrypting encrypted header information, the encrypted header information comprising one or more of an encrypted IP address, an encrypted username of said second computer, an encrypted header length, an encrypted message length, an encrypted application identifier, an encrypted time and date stamp, and an encrypted message type.

72. The method of claim 66, wherein communication between the first computer and the third intermediate computer is initiated by the first computer, and wherein communication between the second computer and the third intermediate computer is initiated by the second computer.

73. The method of claim 66, wherein the first firewall and the second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages transmitted by a computer inside the firewall.

74. A method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall via a third intermediate computer, comprising the steps of:

transmitting a request from the second computer to the third intermediate computer through the second firewall to establish a receive channel between the third intermediate computer and the second computer;

receiving from the third intermediate computer a response to the request, the response establishing a receive channel between the third intermediate computer and the second computer that is to be kept open for subsequent transmissions from the third intermediate computer; and

receiving data via the receive channel, wherein the data was transmitted from the first computer to the third intermediate computer through the first firewall via a network connection

initiated by the first computer, then transmitted from the third intermediate computer to the second computer via the receive channel.

75. The method of claim 74, wherein the request comprises a message transmitted using a secure socket layer (SSL) protocol, a file transfer protocol (FTP), a HyperText Transfer Protocol (HTTP), or an electronic mail protocol.

76. The method of claim 74, wherein the request comprises an HTTP POST message transmitted through the second firewall to port 80 or port 8080.

77. The method of claim 74, wherein the data received via the receive channel comprises an HTTP message from the first computer, the HTTP message encrypted using encryption keys shared between the first computer and the second computer.

78. The method of claim 74, wherein the data received via the receive channel comprises an HTTP message from the first computer, the HTTP message encrypted using encryption keys shared between the third intermediate computer and the second computer

79. The method of claim 78, wherein the encrypted HTTP message comprises encrypted header information including one or more of an encrypted IP address, an encrypted username of said second computer, an encrypted header length, an encrypted message length, an encrypted application identifier, an encrypted time and date stamp, and an encrypted message type.

80. The method of claim 74, wherein communication between the first computer and the third intermediate computer is initiated by the first computer, and wherein communication between the second computer and the third intermediate computer is initiated by the second computer.

81. The method of claim 74, wherein the first firewall and the second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages transmitted by a computer inside the firewall.

EVIDENCE APPENDIX

37 C.F.R. § 41.37(c)(1)(ix)

NONE.

RELATED PROCEEDINGS APPENDIX

37 C.F.R. § 41.37(c)(1)(x)

NONE.